Math100B - HW #5

Jay Ser

2026.02.15

1.

(a)

$x^2 + 1$ factors; $x = 2$ is a root.

$$2^2 + 1 = 5 \equiv 0 \pmod 5$$

(b)

$x^2 - 3x - 3$ factors; $x = 1$ is a root since

$$1^2 - 3(1) - 3 = -5 \equiv 0 \pmod 5$$

(c)

One can brute force check that $x^4 + 2$ has no roots, hence has no degree 1, and thereby no degree 3, factor. Thus if $x^4 + 2$ did factor, it would be of the form

$$x^4 + 2 = (ax^2 + bc + c)(\alpha x^2 + \beta x + \gamma)$$

where the factors can be taken to monic since $\mathbb{Z}/5\mathbb{Z}$ is a field. Muliplying out the factors yields the following system of equations (among more)

$$bd = 2 \tag{1}$$
$$a + c = 0 \tag{2}$$
$$ac + b + d = 0 \tag{3}$$

Modding out symmetric solutions (notice (b, d) have symmetric solutions and (a, c) have symmetric solutions), (1) gives

$$(b, d) \in \{(1, 2), (3, 4)\}$$

If $(b, d) = (1, 2)$, then (3) is equivalent to $ac = 3$, which gives $(a, c) \in \{(1, 3), (2, 4)\}$. But both these solutions contradict (2). If $(b, d) = (3, 4)$, then (3) gives $(a, c) \in \{(1, 2), (3, 4)\}$, both of which contradict (2) once again.

This shows that $x^4 + 2$ has no factors; it is irreducible.

2.

Induct on d, the degree of $f(x) \in F[x]$. If $d = 1$, write $f(x) = ax - b$ with $a \neq 0$. Then $x = ba^{-1}$ is the unique root for f, which proves the base case.

Suppose every polynomial of degree $d-1$ has at most $d-1$ roots, and take any $f(x) \in F[x]$ with degree d. If $f(x)$ has no roots, then there is nothing to be shown. Suppose c is a root of $f(x)$. Then

$$f(x) = (x - c)q(x)$$

where $q(x)$ must be a degree $d-1$ polynomial since F is a field. $q(x)$ has at most $d-1$ roots, so $f(x)$ has at most d roots, as was to be shown.

If F is not a field, then this is not true. For example, in $\mathbb{Z}/4\mathbb{Z}$, the polynomial $g(x) = 2x$ has two roots: 0 and 2.

3.

Suppose there are only finitely many monic irreducible polynomials in $F[x]$. Let this set of irreducibles be

$$\mathcal{F} = \{f_1, f_2, \ldots, f_n\}$$

Take $g(x) = \prod_{i=1}^{n} f_i(x) + 1$. g is clearly monic and not in $\mathcal{F}$, which means it is not irreducible. Since none of the $f_i \in \mathcal{F}$ divide 1 (due to the f_i having a higher degree than the constant 1, for example), none of the $f_i \in \mathcal{F}$ divide $g(x)$. So a monic irreducible factor of g exists, but it is not in the set of all monic irreducible polynomials, which is a contradiction. Thus, $F[x]$ has infinitely many monic irreducible polynomials.

Namely, if F is a finite field, then $F[x]$ has irreducible polynomials of arbitrarily high degree because for any degree d, there are finitely many polynomials of degree d.

4.

(a)

Suppose $\langle 2, x\rangle = \langle f\rangle$ for some $f(x) \in \mathbb{Z}[x]$. Then $f \mid 2$. Since $\mathbb{Z}$ is an integral domain $\implies$ $\mathbb{Z}[x]$ integral domain $\implies$ $\deg(f) \leq \deg(2) = 0$, $f(x)$ must be some constant, say $f(x) = c \in \mathbb{Z}$. But $\langle f\rangle = \langle c\rangle = \langle 2, x\rangle$ says that $c \mid x$, and the only constant that divides x is 1 and -1. So c is a unit, i.e.,

$$\langle 2, x\rangle = \langle c\rangle = \mathbb{Z}[x]$$

But $x + 1$ is clearly not in $\langle 2, x\rangle$, which is a contradiction. Thus $\langle 2, x\rangle$ cannot be principal.

(b)

f is an irreducible element of $\mathbb{Z}[x]$, which is a UFD. An element in a UFD is prime $\iff$ it is irreducible, so f is a prime element of $\mathbb{Z}[x]$. Hence the principal ideal generated by f is prime.

While $\langle f\rangle$ is maximal amongst principal ideals, it is not a maximal ideal. Take any prime number p that doesn't divide the leading coefficint of f. Then by the correspondence theorem,

$$\mathbb{Z}[x]/\langle f(x), p\rangle \cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{\langle \bar{f(x)}\rangle} \tag{1}$$

Since p doesn't divide the leading coefficient of f, $\bar{f}$ has the same degree as f, say n. The units of $\mathbb{Z}/p\mathbb{Z}[x]$ are just the units of $\mathbb{Z}/p\mathbb{Z}$, i.e., the constant 1. $\bar{f}$ has the same degree as f since p doesn't dividie the leading coefficient of f. Namely, $\bar{f}$ is not a constant, so $\langle \bar{f} \rangle$ is not the entire ring $\mathbb{Z}/p\mathbb{Z}[x]$, So (1) is not the zero ring, which means $\langle f(x), p \rangle$ is a proper ideal properly containing $\langle f(x) \rangle$. $\langle f(x) \rangle$ is not a maximal ideal.

5.

(a)

$a + bi$ is a root of

$$q(x) := (x - (a + bi))(x - (a - bi)) = x^2 - 2bx + a^2 + b^2$$

which, by the right hand side, is clearly a degree two polynomial in $\mathbb{R}[x]$.

(b)

Consider the substitution homomorphism

$$\varphi : \mathbb{R}[x] \to \mathbb{C};\ x \mapsto a + bi,\ \varphi|_{\mathbb{R}} = \mathrm{id}$$

It was shown multiple times throughout the course (e.g, the midterm) that $\ker \varphi = \langle q \rangle$. Since $f(a + bi) = 0$ by definition, $f \in \ker \varphi$, which means $q \mid f$.

(c)

For any field F, all degree one polynomials in $F[x]$ are irreducible. If $ax - b = \alpha\beta$, $a \neq 0$, then α or β must be a constant since $\deg(ax - b) = 1 = \deg(\alpha) + \deg(\beta)$.

If $f(x) \in \mathbb{R}[x]$ has degree two, it is irreducible if and only if it has a complex root.

Suppose $f(x)$ has degree greater than two. Since $\mathbb{R}[x] \hookrightarrow \mathbb{C}[x]$, $f(x)$ can be viewed as a complex polynomial. $\mathbb{C}$ is algebraically closed, so $f(x)$ has some root α. If α has no complex part, then $f(x)$ has a linear real factor. If α has a complex part, then by (a) and (b), $f(x)$ has a quadratic factor. Either way, $f(x)$ factors and hence it is not irreducible.

6.

Define the norm function

$$\lambda : \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}_{\geq 0};\ a + b\sqrt{-2} \mapsto a^2 + 2b^2$$

See Q7 for a parallel analysis showing why λ is a multiplicative function: $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, $\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta)$.

Take any $\alpha, \gamma \in \mathbb{Z}[\sqrt{-2}]$, where $\alpha = a + b\sqrt{-2}$ and $\gamma \neq 0$. Since γ is a complex number, $\gamma^{-1} = \frac{\bar{\gamma}}{\gamma\bar{\gamma}} \in \mathbb{Q}[\sqrt{-2}]$, hence $\alpha/\gamma = x + y\sqrt{-2}$ where $x, y \in \mathbb{Q}$. So

$$\exists \delta = c + d\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}] \text{ where } |x - c| \leq 1/2,\ |y - d| \leq 1/2$$

Let $r := \alpha - \gamma\delta \in \mathbb{Z}[\sqrt{-2}]$. Then, because the norm function is multiplicative and $\gamma \neq 0 \implies \lambda(\gamma) \neq 0$, the following analysis holds:

$$\begin{aligned}\lambda(r)/\lambda\gamma &= \lambda(r/\gamma) \\ &= \lambda(x + y\sqrt{-2} - (c + d\sqrt{-2})) \\ &= (x-c)^2 + 2(y-d)^2 \\ &\leq 1/4 + 1/2 \\ &< 1\end{aligned}$$

This shows that $\lambda(r) < \lambda(\gamma)$, so a division algorithm exists for $\mathbb{Z}[\sqrt{-2}]$; it is a Euclidean domain.

7.

Define the following norm function on $\mathbb{Z}[\sqrt{-5}]$:

$$\lambda : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_{\geq 0}; \quad a + b\sqrt{-5} \to a^2 + 5b^2$$

The following calculation shows that λ is a multiplicative function:

$$\begin{aligned}\lambda(a + b\sqrt{-5})\lambda(c + d\sqrt{-5}) &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= a^2c^2 + 25b^2d^2 + 5(b^2c^2 + a^2d^2) \\ \lambda((a + b\sqrt{-5})(c + d\sqrt{-5})) &= \lambda(ac - 5bd + (bc + ad)\sqrt{-5}) \\ &= a^2 - 10abcd + 25b^2d^2 + 5(b^2c^2 + 2abcd + a^2d^2) \\ &= a^2c^2 + 25b^2d^2 + 5b^2c^2 + 5a^2d^2\end{aligned}$$

i.e., $\lambda(\alpha\beta) = \lambda(\alpha)\lambda(\beta)\,\forall\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$.

Suppose $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit. Then $\exists\beta \in \mathbb{Z}[\sqrt{-5}]$ such that $\alpha\beta = 1$. Applying the norm on both sides of the equality yields

$$\lambda(\alpha)\lambda(\beta) = 1$$

Since λ maps to the nonnegative integers, $\lambda(\alpha) = 1$.

Conversely, suppose $\lambda(\alpha) = 1$. Write $\alpha = a + b\sqrt{-5}$. Notice that $\lambda(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5})$; $a - b\sqrt{-5}$ is α's inverse; This shows that $\alpha \in \mathbb{Z}[\sqrt{-5}]$ is a unit $\iff \lambda(\alpha) = 1$.

The norm function gives an easy method way of checking that 2, 3, and $1 \pm \sqrt{-5}$ are all irreducible. Suppose $2 = \alpha\beta$. Applying norm to both sides yields

$$4 = \lambda(\alpha)\lambda(\beta)$$

Since λ maps to nonnegative integers,

$$(\lambda(\alpha), \lambda(\beta)) \in \{(2,2), (1,4), (4,1)\}$$

One can easily check from the definition of the norm function that 2 is not in the image of λ, so either $\lambda(\alpha) = 1$ or $\lambda(\beta) = 1$. Thus one of the factors must be a unit, hence 2 is irreducible. One can use this same method to verify that the 3 and $1 \pm \sqrt{-5}$ are irreducible.

- $3 = \alpha\beta \implies (\lambda(\alpha), \lambda(\beta)) \in \{(3,3),(1,9),(9,1)\}$, but 3 is not in the image of λ.
- $1 \pm \sqrt{-5} = \alpha\beta \implies (\lambda(\alpha), \lambda(\beta)) \in \{(2,3),(3,2),(1,6),(6,1)\}$, but 2 and 3 are not in the image of λ.

Although 2 is an irreducible element, it is not a prime element of $\mathbb{Z}[\sqrt{-5}]$.

$$2 \mid 6 = (1+\sqrt{5})(1-\sqrt{5}), \text{ but } 2 \nmid 1+\sqrt{5}, 1-\sqrt{5}$$

$\mathbb{Z}[\sqrt{-5}]$ is Noetherian, so irreducible decomposition exists. However, because irreducible elements are not neccessarily prime, irreducible decompositions are not unique. This shows $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

8.

(a)

$\mathbb{Z}$ is a famous Euclidean domain that isn't a field.

(b)

By Q4, $\mathbb{Z}[x]$ is a UFD that is not a PID.

(c)

By Q7, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. It is an integral domain, however. Observe

$$(a+b\sqrt{-5})(c+d\sqrt{-5}) = 0 \iff ac = 0,\ bd = 0,\ ad+bc = 0 \tag{1}$$

For any $a, b, c, d \in \mathbb{Z}$. To show that $\mathbb{Z}[\sqrt{-5}]$ is a UFD, it must be shown $(a,b) = (0,0)$ or $(c,d) = (0,0)$. Well, since $\mathbb{Z}$ is an integral domain, the right-hande side of (1) shows $a = 0$ or $c = 0$ and $b = 0$ or $d = 0$. Suppose $a = 0$ and $d = 0$. Then $bc = 0$ and thus $b = 0$ or $c = 0$, thus either $(a,b) = (0,0)$ or $(c,d) = (0,0)$. Similarly, if $b = 0$ and $c = 0$, $ac = 0$, so once again, one of the pairs has to be $(0,0)$. This shows that $\mathbb{Z}[\sqrt{-5}]$ is an integral domain.